Brace168

October 2020 Newsletter

IN THIS ISSUE:

Brace168 Pty Ltd

Level 2, 157 Walker St,
North Sydney

www.brace168.com

info@brace168.com

P: (02) 9136 6066

> "If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you."
>
> - Stephane Nappo

Brace168 News!

We're Growing!!

Welcome to the Brace168 Team

It has been a busy month for new faces as Brace168 continues to enjoy growth through the back half of 2020. Here is a little bit of info about our new starters.

1) Stuart Cam, Software Engineer

"…software developer with 20+ years experience, arriving from Elastic where I was helping build Elasticsearch. I am a keen musician and craft beer enthusiast - often at the same time"

2) Helen Triantis, Senior Account Manager

"…a Melbourne girl with many years of sales experience in the IT industry. I also wear a number of other hats like being a Mum, a psychologist, a doctor, a housekeeper, a chef, a comedian and a peace worker to two children 17 & 22 year-olds. I'm also secretary of a body corp, a basketball manager and I'm even a FIBA accredited basketball statistician. I love a good party and a good laugh! I'm also a pretty good practical joker....so watch out!!"

3) Sheryl Lubke, Finance Administrator

"…. has been working for SMEs for over 13 years and I thoroughly enjoy the close-knit relationships that the small business environment offers. I am currently completing a Masters Degree in Professional Accounting at Macquarie University.

An interesting thing about me is that I never learnt to swim despite growing up and living 20 steps (could be 30 steps) away from the beach "

Stuart, Helen and Sheryl collectively bring a wealth of experience to Brace168.

Jump into the LinkedIn comments section and help us welcome them to the Brace168 family.

Brace168's thoughts on

Industry News!

What is Cyber Resilience?

Cyber resilience refers to the ability of a business to continuously deliver their intended outcome, despite adverse cyber events. An organization has cyber resilience if it can defend itself against cyber events, limit the effects of a security incident, and guarantee the continuity of its operation during and after the events. These events may be intentional (e.g. cyber attack) or unintentional (e.g. failed software update) and caused by humans, IT systems, or a combination of both!

Why is cyber resilience important?

1) **Enhancing system security:** It also helps boost safety and security across the system and decreases the possibility of cyberattacks.
2) **Reducing financial losses:** Regardless of how good the IT security of an organization, the fact is that no entity is immune to cyberattacks. If an organization has cyber resilience, the effect of the attack will be lessened, and so is the financial losses.
3) **Getting regulatory and legal requirements:** Meeting legal requirements is also a valuable benefit in integrating cyber resilience in an organization.
4) **Enhancing work culture and internal process:** When people are inspired to take security seriously in their organization, sensitive information and physical assets are more likely in good hands.
5) **Protecting an organization's reputation:** Cyber resilience prevents an organization from public scrutiny, fines from regulators, and an abrupt reduction in sales, or worse, loss of business.

Now cyber resilience sounds like a great idea, but in order to achieve a secure business environment, it may take years of implementing cyber security products and managed services tailored to your unique needs. Your business could end up with a 3, 5 or 10 year plan! However, we live in the real world, and **hackers will not wait for your business to finish its cyber plan before they attack**. That is why an **Accelerated Cyber Resilience Program** is extremely valuable in today's climate. Brace168 will scope your unique security posture, prioritise security measures based on degree of urgency, and implement them in an evolving, front-heavy timeline that is adaptive to threats as they appear. In doing so, you protect your business from critical threats early, and then adjust for lower level threats towards the end of the timeline.

Who's currently doing this?

Toll Group is taking its first major action since recovering from two devastating ransomware attacks, outlined in previous newsletters this year, by kicking off a one year "accelerated cyber resilience program".

CIO King Lee – "The world has totally changed from the beginning of 2020. We are adapting well in the current remote working environment, but we need to think further and move faster to create a better future that's exciting, innovative and safe."

Common Vulnerabilities & Exposure for October

1. An authentication bypass vulnerability has been found in the Netlogon Remote Protocol, which is an interface that Windows uses to authenticate users and computers on domain-based networks. The vulnerability, named Zerologon, allows attacker to impersonate any computer to the domain controller and change their password, including the password of the domain controller itself. This results in an attacker gaining administrative access and taking full control of the domain controller and therefore the network. Exploitation of this vulnerability poses a complete loss of confidentiality, integrity and availability. The US Department of Homeland Security determined that this vulnerability poses an unacceptable risk and immediate emergency action is required.
    - CVE-2020-1472

Score: 10 - Critical

Likelihood: Critical – Microsoft's threat intelligence team have observed attackers targeting the vulnerability using publicly available exploits which has drastically heightened the risk. Threat actors are actively scanning for unpatched servers to exploit.

Recommendation: Patch all versions of Windows Server. Where patches cannot be performed, organisations should ensure logging is enable for the following events:

- **Event ID 4624; 4742** – An account was successfully logged on, or A computer account was changed;
    - **Security ID:** ANONYMOUS LOGON
    - **Account Name:** ANONYMOUS LOGON
    - **Account Domain:** NT AUTHORITY

If a system is patched, monitor:

- **Event ID 5827, 5828, and 5829 –** Events related to insecure connection attempts that are denied;
- **Event ID 5830, and 5831 –** Events related to insecure connection attempts that are successful.

Brace168 can handle your log ingestion and provide real-time incident response.

2. There is a remote code execution vulnerability for Bluetooth on Android devices. The vulnerability, named BLURtooth, allows an attacker to manipulate the CTKD component to overwrite other Bluetooth authentication keys on a device, and grant an attacker connecting via Bluetooth access to other Bluetooth-capable services/apps on the same device. As such, a man-in-the-middle attack could be used to execute code remotely on linked devices. Exploitation of this vulnerability poses a potential loss to confidentiality, integrity and availability.
    - CVE-2020-0354
    - CVE-2020-15802

Score: 9.8 - Critical

Likelihood: Low –Since the threat actor needs to be within 250m of the target, it is ultimately unlikely to be exploited. However, exploits are in the wild and have been automated such that you could be automatically connecting to a threat actor on your way home from work without even knowing about it.

Recommendation: Update Bluetooth. It is important to understand how all devices in your organization are connected and how they can be used in an attack. Brace168 can monitor Intune logs to give you better visibility to the mobile devices in your organisation that are often ignored!